

The Honorable Robert S. Lasnik

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff

v.

PAIGE A. THOMPSON,

Defendant.

NO. CR19-159 RSL

**UNITED STATES' SUPPLEMENTAL
FILING RELATING TO
DEFENDANT'S MOTION TO STRIKE
CRYPTOJACKING ALLEGATIONS
AND TO SEVER COUNT 8**

Defendant, Paige Thompson, has filed a motion to strike from Count 1 the allegation that she engaged in cryptojacking and to sever Count 8, which charges her with damaging protected computers by engaging in cryptojacking and deleting records of that cryptojacking. *See* Docket No. 124. As part of her reply in support of her motion, Thompson argues that the Court should grant the motion because there supposedly is no evidence that Thompson used servers belonging to Victim 7 and Victim 8, both of which also were victims of Thompson's data theft, to perform cryptojacking. *See* Docket No. 163, at 6-8.

Thompson's filing misstates the record. First, as the exhibits to Thompson's reply make clear, Victim 7 had unauthorized virtual servers created on its account that resulted in it being billed more than \$40,000 by Amazon Web Servers (AWS). *See* Docket No.

1 163, Ex. 3, at 2. Although, Victim 7 was unable to determine that these were used for
2 cryptocurrency mining (because Thompson’s scripts deleted the unauthorized software
3 and related logs), it is significant that this occurred during the timeframe in which
4 Thompson was hacking AWS clients, including Victim 7. It also is significant that the
5 unauthorized commands “came from an AWS IAM role” that was “associated with
6 [Victim 7’s] instance,” *See id.* at 1. This is the exact attack vector used by Thompson.
7 This obviously is evidence that Thompson used Victim 7’s rented servers at AWS to
8 conduct cryptocurrency mining.

9 Second, although Thompson’s reply does not mention it, Thompson’s counsel
10 asked the government, in April 2021, to identify discovery supporting the allegation that
11 Thompson used victim servers to engage in cryptocurrency mining. In response, the
12 government provided a detailed summary of forensic evidence from Thompson’s seized
13 computers that showed that Thompson engaged in such activity. (That response is
14 attached as Exhibit A to this filing.) The response identifies various computer scripts that
15 Thompson used to conduct this activity. In particular, it identifies scripts used to plant
16 cryptocurrency-mining software on Victim 8’s rented servers at AWS.

17 As a result, there is (and Thompson has been provided) evidence that shows that
18 she used servers of both Victim 7 and Victim 8 to conduct cryptocurrency mining. For

19 //

20 //

21 //

1 the foregoing reasons, as well as those stated in the government's original opposition to
2 Thompson's motion, the Court should deny the motion.

3 DATED: January 14, 2022.

4
5 Respectfully submitted,

6 NICHOLAS W. BROWN
7 United States Attorney

8 s/ Andrew C. Friedman
9 ANDREW C. FRIEDMAN
10 JESSICA M. MANCA
11 Assistant United States Attorneys
12 700 Stewart Street, Suite 5220
13 Seattle, Washington 98101
14 Phone: (206) 553-7970
15 Fax: (206) 553-0882
16 E-mail: Andrew.Friedman@usdoj.gov
17 Jessica.Manca@usdoj.gov
18
19
20
21
22
23
24
25
26
27
28